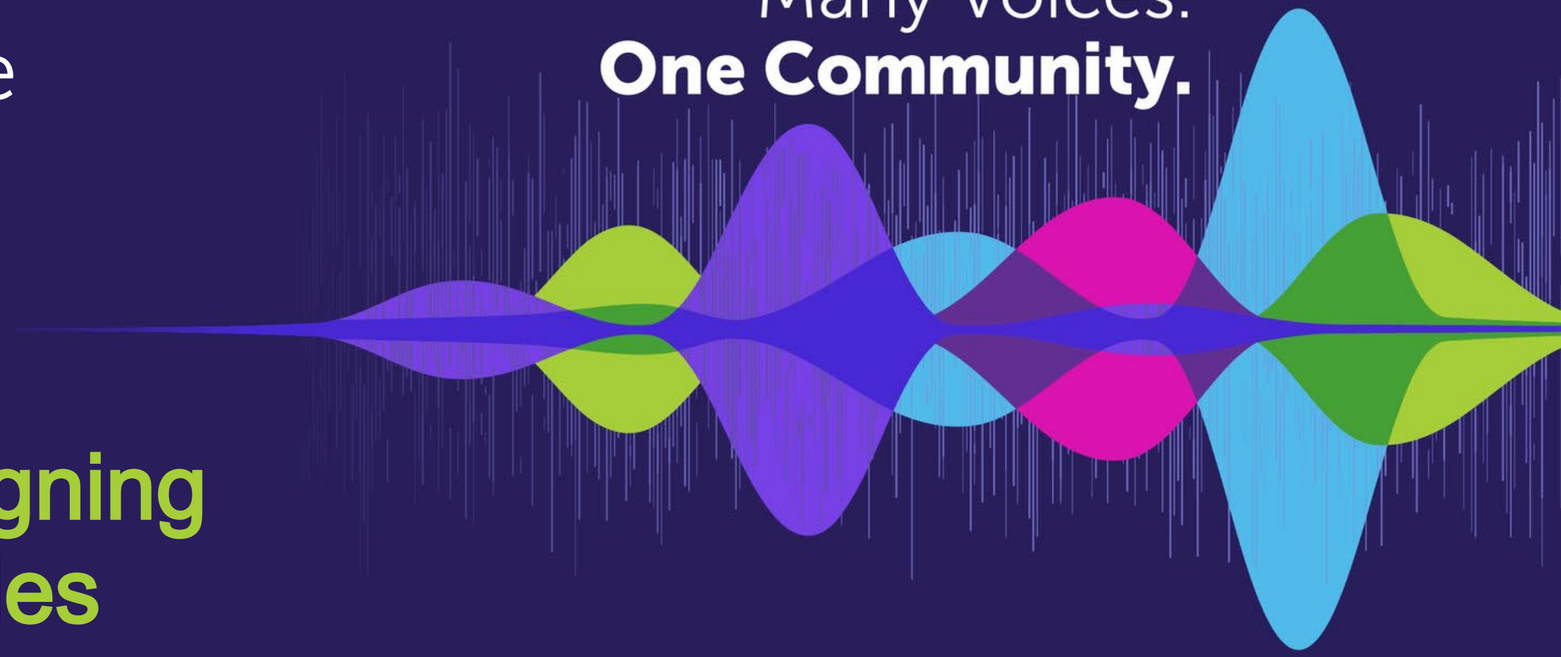
RSAC | 2025 Conference

Many Voices.
One Community.



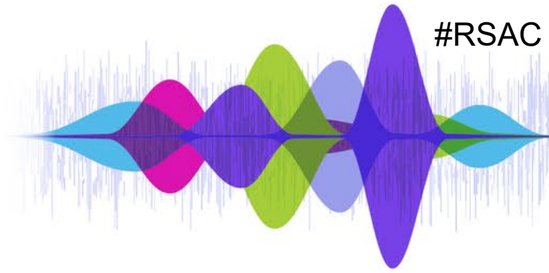
SESSION ID:
ICWD-W08

NICE to Meet You: Aligning Talent to the Right Roles

Derek Fisher

Director of the Cyber Defense and Information Assurance Program @ Temple University
Founder of Securely Built

linkedin.com/in/derek-fisher-sec-arch/



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

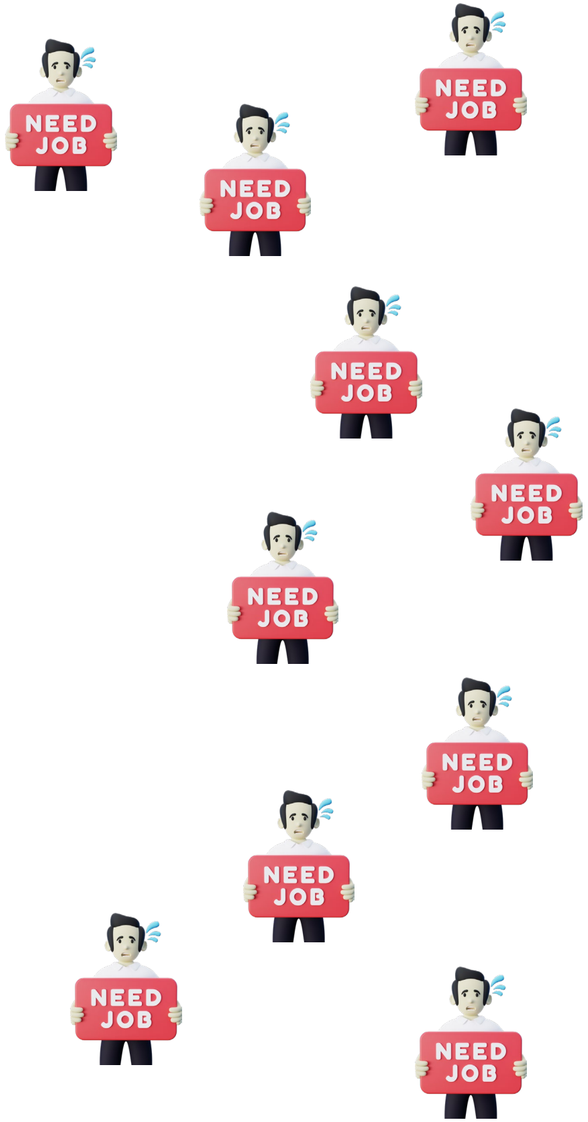
Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Who’s looking for work?

Bob is searching far and wide for a role in cybersecurity….

This is Bob



Expectations

Reality

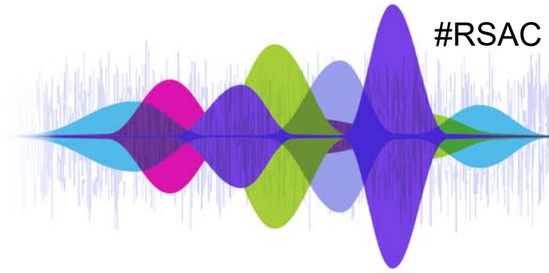
The numbers are everywhere....

REALITY ?

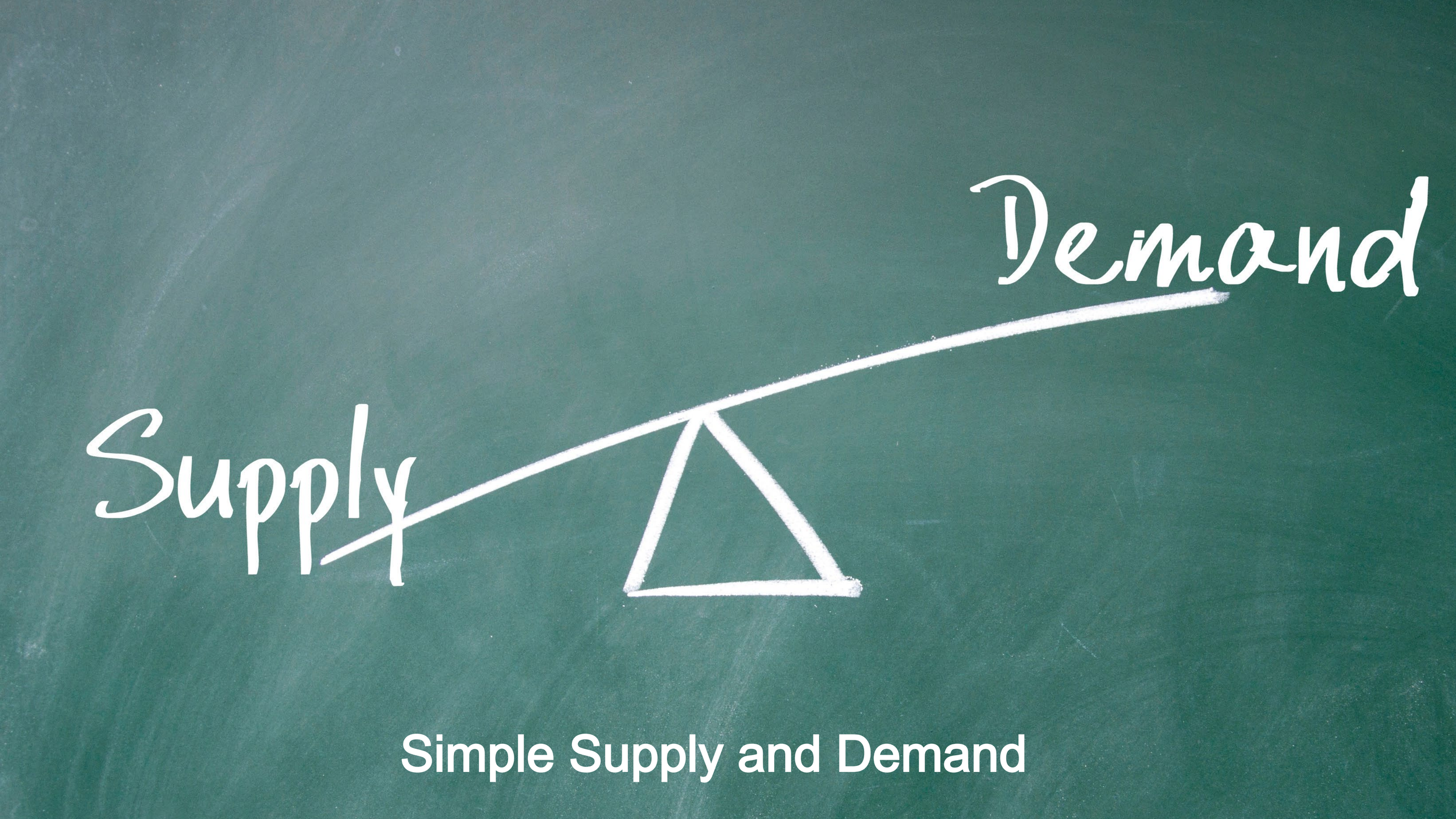
NEED
JOB

Job description:

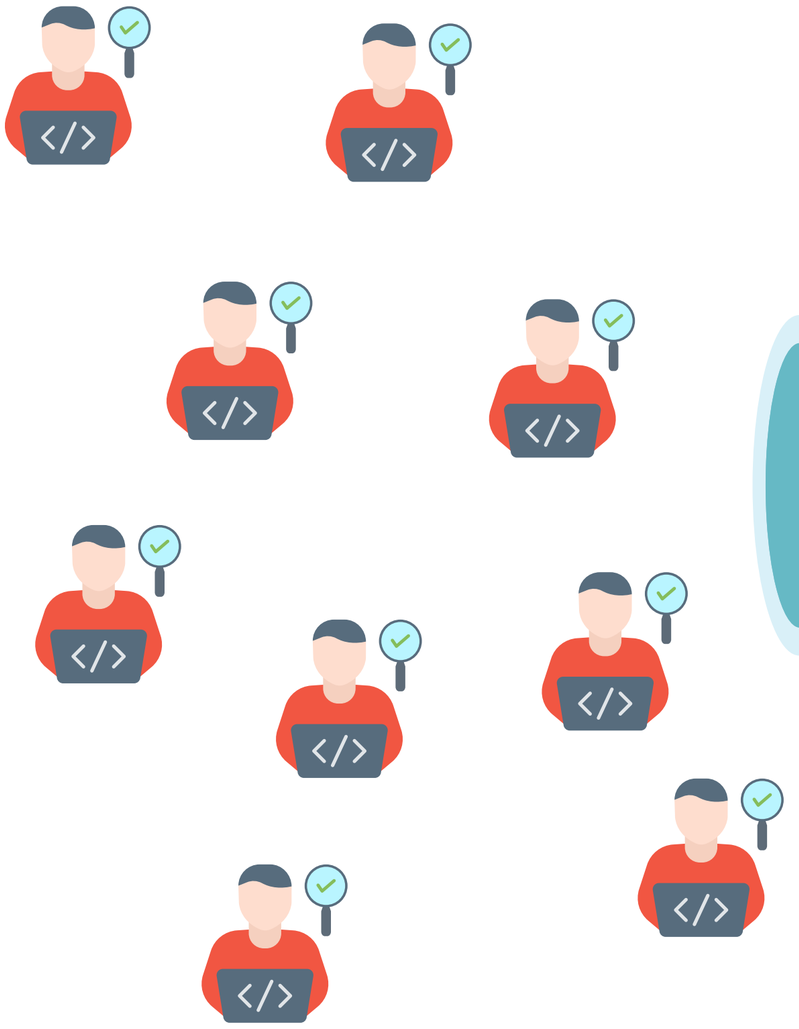
JOB MARKET
Local ads in print and online

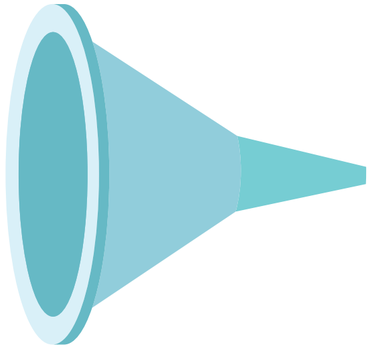


Problem 1

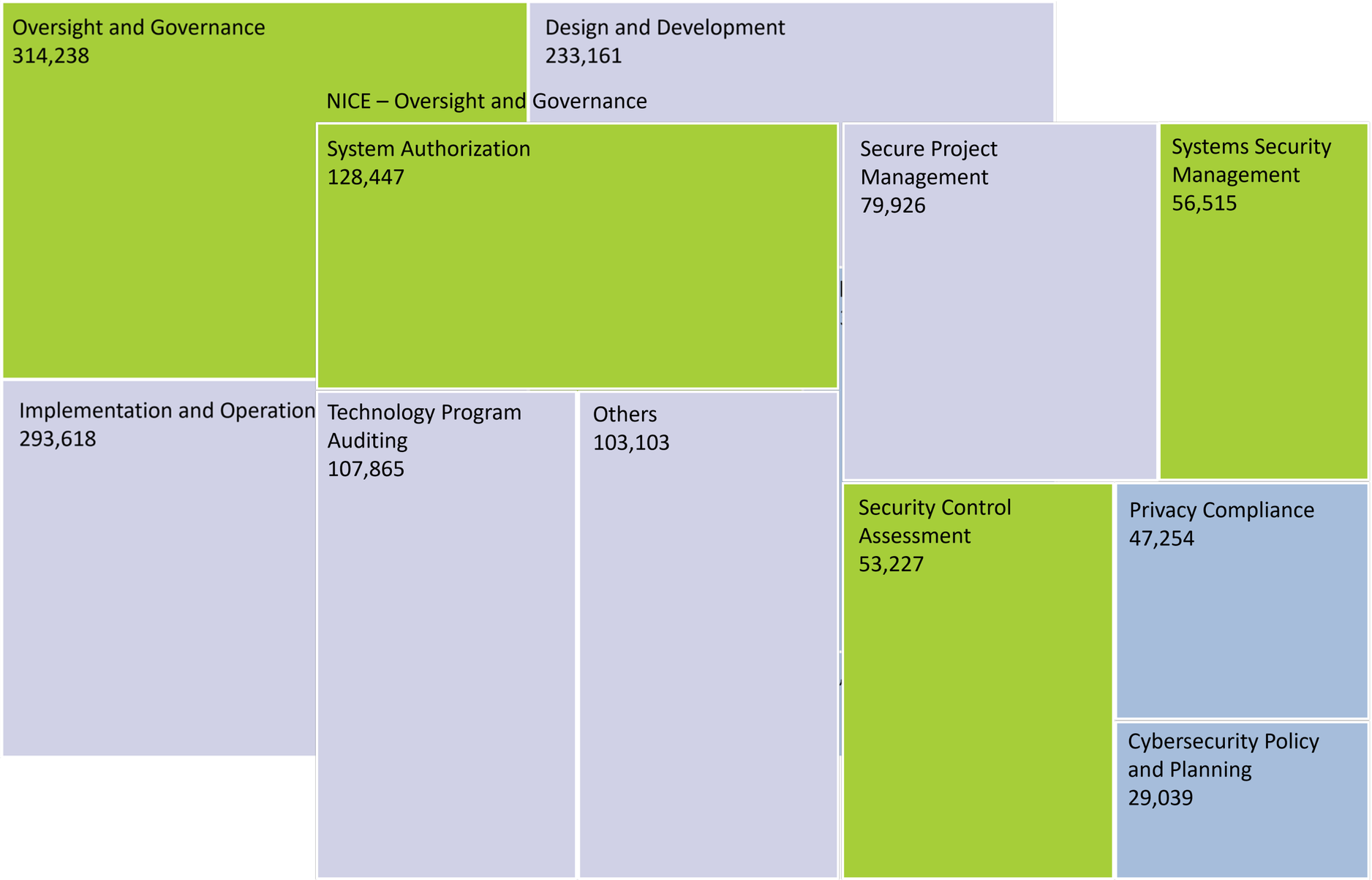


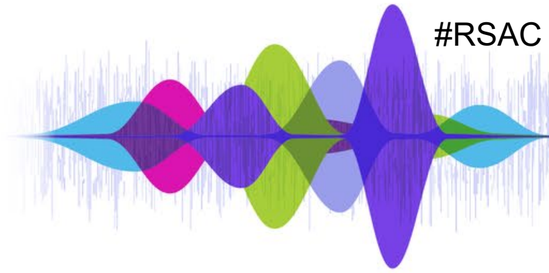
Simple Supply and Demand





Per ZipRecruiter there are 6,495 Penetration Tester Jobs (Mar 2025)


Oversight and Governance
314,238
Design and Development
233,161
NICE – Oversight and Governance
System Authorization
128,447
Secure Project Management
79,926
Systems Security Management
56,515
Implementation and Operation
293,618
Technology Program Auditing
107,865
Others
103,103
Security Control Assessment
53,227
Privacy Compliance
47,254
Cybersecurity Policy and Planning
29,039



Problem 2

Misaligned on skills & experience

Poorly Written
Job Descriptions
imgflip.com

I need a job description for....

Secure Systems Development

Responsible for the secure design, development, and testing of systems and the evaluation of system security throughout the systems development life cycle.

Key responsibilities:

Security Requirements Analysis:

- Identify and document security requirements for new systems, including threat modeling and risk assessment to prioritize security concerns.

Secure Design:

- Design system architectures with security in mind, incorporating encryption, authentication, authorization, and access controls.

Secure Coding Practices:

- Implement secure coding standards and best practices to minimize vulnerabilities within the application code.

Vulnerability Assessment and Penetration Testing:

- Conduct regular security testing to identify potential vulnerabilities and weaknesses in systems and applications.

Required Skills:

Programming Languages:

- Proficiency in relevant programming languages used for system development (e.g., Java, Python, C++)

Security Concepts:

- Deep understanding of security principles like cryptography, authentication, authorization, access control, and vulnerability management

Security Testing Methodologies:

- Experience with various security testing techniques (e.g., penetration testing, code review, fuzzing)

System Architecture:

- Knowledge of system architecture design principles and how to incorporate security considerations

Reality – Sample Job Description

Not awful, but pretty generic…

Secure Systems Development

Responsible for the secure design, development, and testing of systems and the evaluation of system security throughout the systems development life cycle.

Standard skills and blanket security certificates

Poorly crafted generic job description

There has to be a better way!

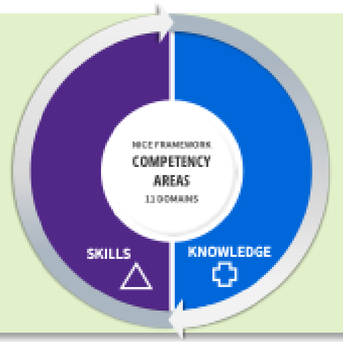
NICE
TO MEET
YOU!

What is the NICE Framework Competency

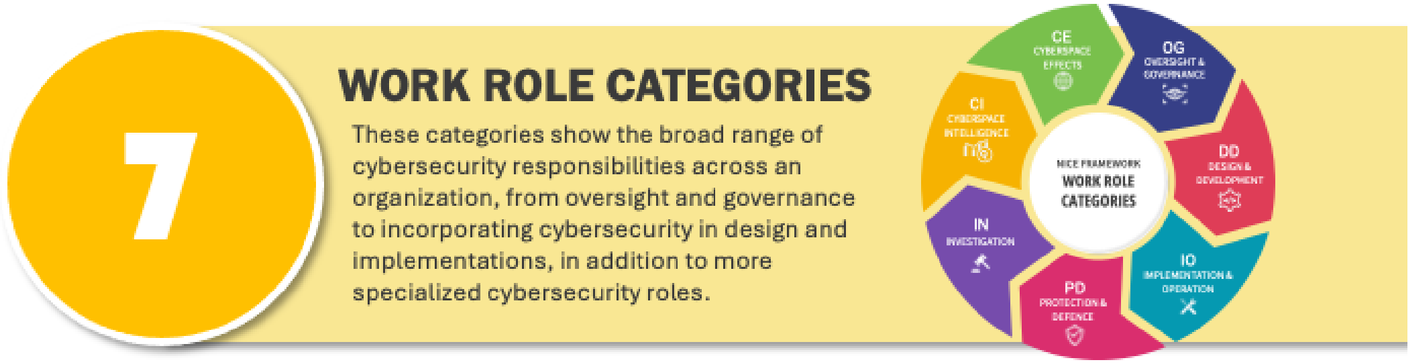
11

COMPETENCY AREAS

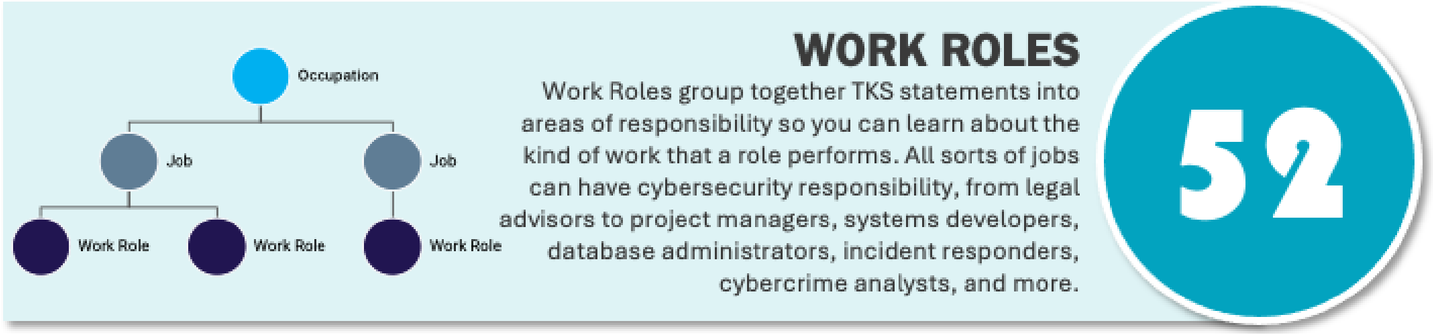
Competency Areas focus on a learner's capabilities in particular domains. These can be used in conjunction with Work Roles or on their own and represent emerging areas and other topics such as AI Cybersecurity, Cyber Resiliency, Operational Technology Security, and Supply Chain Security.



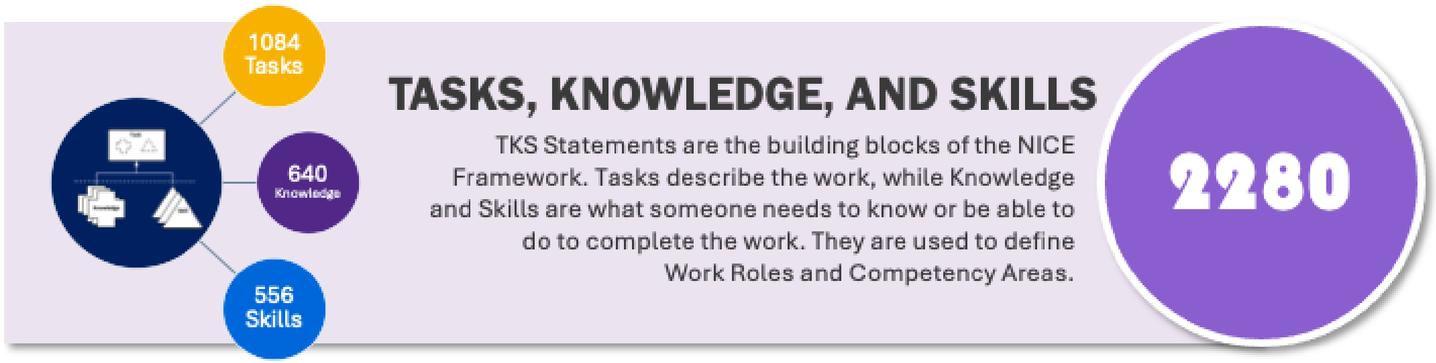
What is the NICE Framework Work Role Categories



What is the NICE Framework Work Roles


Occupation
Job
Job
Work Role
Work Role
Work Role
WORK ROLES
Work Roles group together TKS statements into areas of responsibility so you can learn about the kind of work that a role performs. All sorts of jobs can have cybersecurity responsibility, from legal advisors to project managers, systems developers, database administrators, incident responders, cybercrime analysts, and more.
52

What is the NICE Framework TKS


1084
Tasks
640
Knowledge
556
Skills
TASKS, KNOWLEDGE, AND SKILLS
TKS Statements are the building blocks of the NICE Framework. Tasks describe the work, while Knowledge and Skills are what someone needs to know or be able to do to complete the work. They are used to define Work Roles and Competency Areas.
2280

Secure Systems Development

Responsible for the secure design, development, and testing of systems and the evaluation of system security throughout the systems development life cycle.

Role Summary

As an Enterprise Security Architect, you will be responsible for designing, implementing, and overseeing the organization's comprehensive cybersecurity strategy and architecture. You will serve as a key advisor to senior management on risk levels, security posture, and cybersecurity initiatives while ensuring compliance with relevant laws and regulations. This role requires expertise in communications security, encryption technologies, risk management, and business continuity planning to protect the organization's critical assets and infrastructure.

Key Responsibilities

- Advise senior management on risk levels, security posture, and organizational cybersecurity efforts
- Establish and maintain the enterprise information security architecture
- Develop and implement the enterprise continuity of operations strategy and program
- Identify, report, and respond to cybersecurity and COMSEC incidents
- Implement protective or corrective measures when cybersecurity incidents or vulnerabilities are discovered
- Determine operational and safety impacts of cybersecurity lapses
- Perform cost/benefit analyses of cybersecurity programs, policies, processes, systems, and elements
- Review enterprise IT goals and objectives to ensure alignment with security requirements
- Identify critical technology procurement requirements and evaluate security designs
- Identify roles and responsibilities for appointed COMSEC personnel
- Communicate the value of cybersecurity to organizational stakeholders
- Validate implementation of security improvement actions

Required Qualifications

- Demonstrated knowledge of cybersecurity principles, practices, threats, and vulnerabilities
- Experience with encryption algorithms, PKI, and digital signatures
- Proficiency in implementing enterprise key escrow systems and network communication encryption
- Strong understanding of communications security (COMSEC) policies, procedures, and incident types
- Knowledge of risk management principles, processes, and practices
- Experience with business continuity and disaster recovery (BCDR) planning
- Understanding of systems security engineering (SSE) principles
- Knowledge of computer networking principles and network security
- Ability to perform cost/benefit and risk analyses
- Experience implementing security system controls
- Understanding of data classification standards and data security controls
- Knowledge of applicable cybersecurity and privacy laws and regulations
- Experience auditing technical systems and identifying security violations
- Understanding of supply chain risk management principles

NEED
JOB

Secure Systems Development

Responsible for the secure design, development, and testing of systems and the evaluation of system security throughout the systems development life cycle.

Skills to Develop:

- Encryption & PKI Management: Implement and manage PKI, key escrow, digital signatures, and network encryption protocols like TLS, IPsec, and VPNs.
- Security Architecture: Design enterprise security frameworks, Zero Trust models, cloud security, and identity and access management solutions.
- Risk Management: Perform risk assessments, business impact analysis, cost-benefit evaluations, and develop security metrics and KPIs.
- Compliance & Governance: Navigate regulatory frameworks, create security policies, conduct audits, and perform gap analyses.
- Communications Security: Apply COMSEC principles, secure communication protocols, data classification, and data loss prevention (DLP) strategies.

Essential and Advanced Certifications

- CISSP, CISM, SABSA, CCSP, CRISC

Training and Education

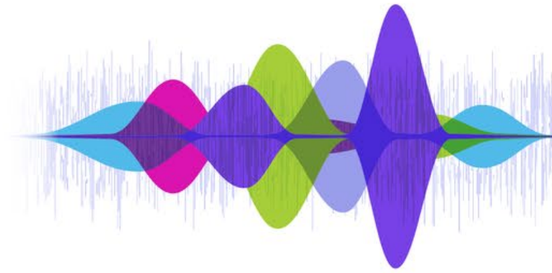
- Formal Education: Degrees in Cybersecurity, Computer Science, or Information Systems, with advanced coursework in security architecture and engineering.
- Specialized Training: SANS courses, cloud security certifications (AWS, Azure, GCP), and risk management framework training (NIST RMF, ISO 31000).
- Workshops & Bootcamps: Hands-on learning through incident response exercises, business continuity workshops, and security architecture labs.

Building Experience

- Career Progression: Begin in security operations or compliance, advance to engineering roles, manage security projects, and gradually take on architect responsibilities.
- Volunteer Opportunities: Contribute to non-profits, open-source security projects, or industry working groups to build experience.
- Document Your Work: Create case studies, document architectural decisions, and build a portfolio showcasing your design patterns.
- Industry Engagement: Present at conferences, publish articles or white papers, and stay active in professional security communities.

Show and Tell Experience

- Security Architecture Portfolio: Design a full security architecture for a fictional organization, including diagrams, control matrices, and implementation plans across key security domains.
- Risk Assessment Project: Perform a risk assessment with quantitative analysis, controls mapping, remediation plans, and executive-level reporting.
- Encryption Implementation: Build a lab-based PKI setup with documented key management and certificate lifecycle processes.
- Policy Framework Development: Develop a complete security policy framework with implementation guidelines, metrics, and regulatory alignment.
- Business Continuity Plan: Create a BCP/DR strategy with recovery procedures, testing methods, and tabletop exercise scenarios.



Secure Systems Development

SUCCESS

Apply - Job Seekers

Determine your path and what your answer is to “what do you want to do?”

Align to the skills, knowledge, and tasks in the NICE framework for the role you are chasing

Build those skills in a demonstrable way (repo, project work, open source, etc...)

Apply – Hiring Teams

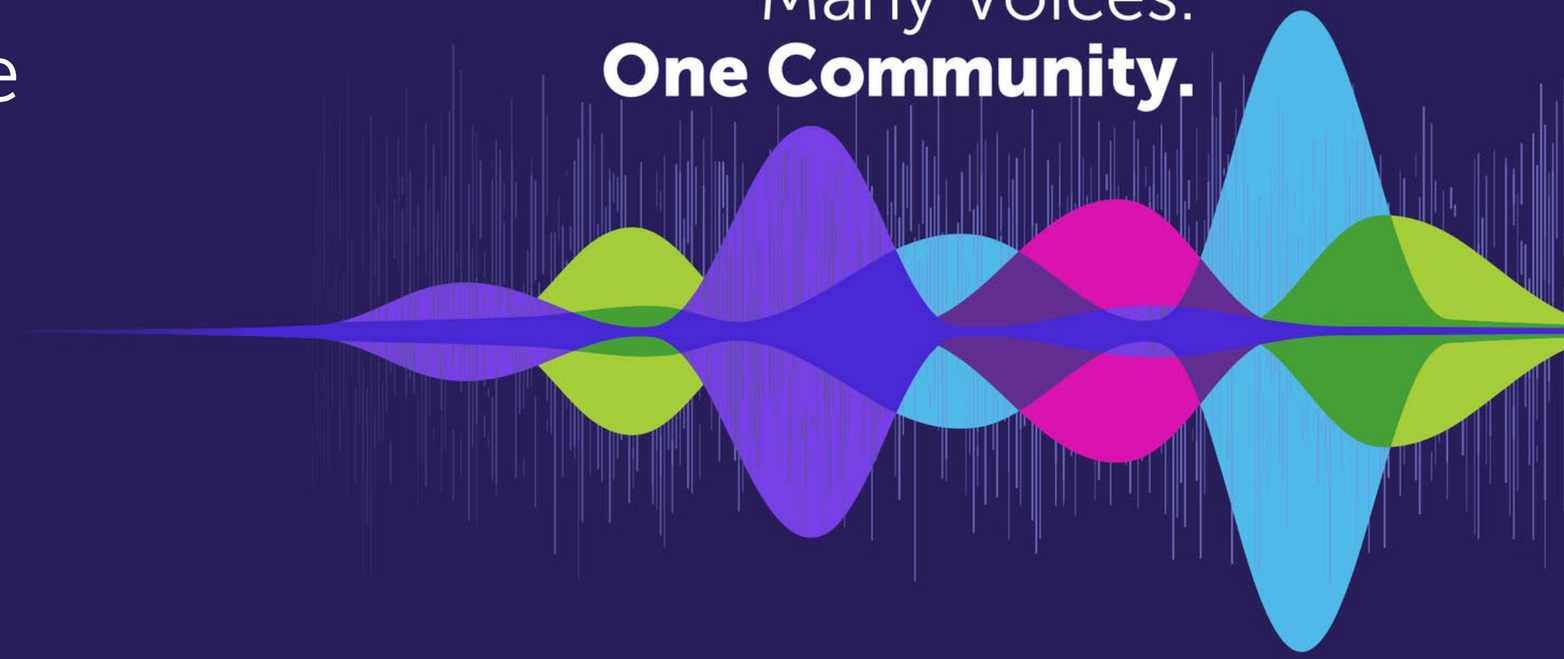
Know what you need for the role

Review the NICE framework and understand the task, knowledge, and skills required

Build a job description that accurately reflects the need and aligns to NICE

RSAC 2025 Conference

Many Voices.
One Community.



SESSION ID:

Thank you!

Derek Fisher

Director of the Cyber Defense and Information Assurance Program @ Temple University
Founder of Securely Built

linkedin.com/in/derek-fisher-sec-arch/